Partial Translation of Japanese Unexamined Patent Publication (Kokai) No. 06-168114

Date of publication: June 14, 1994
Application number: 04-319530
Date of filing: November 30, 1992

Title of the Invention: COMPUTER VIRUS PROTECTION APPARATUS

Applicant: Japan System Project Co., Ltd.
Inventor: Tatsuhiko Tsuchiya

1. Paragraph Numbers [0007] to [0011] in "Detailed Description of the Invention"

[0007]

[Problems to be Solved by the Invention] As described above, a computer virus infects a computer system via the use of a program infected with the virus or via computer communications, etc. Once it has infected the computer system, it causes various adverse effects on the computer system. One way to prevent the intrusion of computer viruses would be to use only credible programs but, since there are viruses that intrude via computer networks, it is not possible to perfectly prevent their intrusion, and the computer system may become infected from an unexpected source. Further, the reality is that there is no way to prevent viruses from intruding via computer communications.

[0008]

Furthermore, at the present state of the art, to check a file for infection, the file must be loaded into the computer system to examine the contents of the file; at this time, the computer system is exposed to a high risk of infection.

[0009]

That is, the virus infection check must be made at

least on the floppy disk level or on the external storage device level, and a suspected file stored on such an external storage device is read out and checked for any change in file size, date, or data sequence to determine if there is a suspicion that the file is infected with a virus. Since, at this time, at least a portion of the file is loaded into the main memory of the computer, even if the readout file is not executed, it is not possible to completely eliminate the possibility of other files in the computer system becoming infected with a virus that may have intruded into the main memory. With regard to worms, on the other hand, since worms propagate through a computer network and infect networked computers, at the present state of the art it is not possible to eliminate such worms.

[0010]

Accordingly, it is an object of the present invention to provide a computer virus protection apparatus that can check a file for a computer virus before the file is read into a computer, thereby preventing a computer virus infection safely and easily.

[0011]

[Means for Solving the Problems] To attain the above object, the present invention provides the following configuration. That is, the invention comprises an external storage means having a removable storage medium; a processing means having a first function for checking a file read out of the external storage means to see if the file is infected with a computer virus, and a second function for performing a cleaning process for eliminating any effect of the computer virus if the file is infected;

and means for writing the cleaned file back to the external storage means.

2. Paragraph Numbers [0029] to [0042] in "Detailed Description of the Invention"

[0029]

The scanning process is a process for executing the scan vaccine program loaded into the memory 17 and for checking the target file in the memory 17 to see if a computer virus is hidden therein. In this case, if anything suspicious or any particular virus is found as a result of the check, the indicator lamp 12-4 corresponding to the clean button 13-4 is flashed to indicate that the file is suspected of being infected with a virus, thus prompting the operator to press the clean button 13-4, and when the clean button 13-4 is pressed, the cleaning process is performed by the clean vaccine program to disinfect the virus-infected file in the memory 17 (which includes removing the virus program portion), and when the cleaning is successfully done, the disinfected file is written to the floppy disk.

[0030]

The RAM is also used as a program work area, a communication buffer, etc. The floppy disk drive 11 has a function for detecting the insertion/removal of the floppy disk.

[0031]

In the above system, the processing described above is performed by reading the attribute of the floppy disk having the scan attribute that provides the scan vaccine program or the clean vaccine program and the attribute of the floppy disk formatted to a specific OS, such as MS-DOS

or DOS/V, that can be handled by the system.

[0032]

The scan vaccine program is a program and data that checks for various kinds of computer viruses and that contains information such as the code sequences of various kinds of currently known computer viruses and the file lengths, file stamps, and file attributes of various well-known software applications and, by making comparisons against these pieces of information, the program identifies a computer virus or checks for the presence of a file suspected of being infected with a compute virus.

[0033]

The clean vaccine program is a virus disinfection program written for each specific known computer virus, and is executed to render a computer virus harmless in a file infected with the computer virus or removes the program routine of the computer virus.

[0034]

Next, the operation of the apparatus having the above configuration will be described with reference to the flowchart of Figure 3. In this apparatus, when a floppy disk is inserted in the floppy disk drive 11, the CPU 14 examines the attribute of the floppy disk (S11, S12). The following processing is performed according to the attribute.

[0035]

If the CPU 14 recognizes that the attribute of the inserted floppy disk is the scan attribute, the CPU 14 reads out a program file and a data file from the floppy disk, and stores them in a specified area within the memory 17 (the scan program area in the case of the scan program,

and the clean program area in the case of the clean program) (S13). When the program is loaded, the process is terminated.

[0036]

On the other hand, if the CPU 14 recognizes that the attribute of the inserted floppy disk is not the scan attribute, but the attribute of a specific OS that can be handled by the system, the CPU 14 turns on the lamps corresponding to the transmit button 13-2 and the scan button 13-3 to notify the operator that the operation for scanning (virus check) is ready to be performed (S21). Next, the CPU 14 monitors whether any one of the buttons indicated by the lamps is operated (S22 to S24).

[0037]

Here, if neither button is pressed, and if data is received from a remote party via the communication interface, such as a modem or an RS232C, then a receive mode is entered and, after linking to the remote end by performing protocol control for reception, the data transmitted from the remote end is received and written to the specified data storage area (work area) within the RAM in the memory 17 (S51). In this state, button operations other than the reset button are not accepted. In this receiving process, the received data written to the memory 17 is written to the floppy disk. When the receiving process is completed, the CPU 14 again monitors whether or not any one of the buttons indicated by the lamps is operated (S23 to S25).

[0038]

If the transmit button 13-2 is pressed, the transmitting process is initiated (S52). In this

transmitting process, protocol control for transmission is performed, after which the file stored on the floppy disk is read out and sent to the RS232C interface or the modem.
[0039]

If the scan button 13-3 is pressed, the scan process is initiated (S25). In this process, the CPU 14 reads out the program file and data file from the floppy disk, and stores them in the specified area (work area) within the memory 17. This is the case in which there are such files stored on the floppy disk; if there are no files stored, the process is terminated.
[0040]

When the files are loaded, the scan program loaded into the memory 17 is executed to check the target file in the memory 17 to see if a computer virus is hidden therein. If anything suspicious or any particular virus is found as a result of the check, the indicator lamp 12-4 corresponding to the clean button 13-4 is flashed to indicate that the file is suspected of being infected with a virus, thus prompting the operator to press the clean button 13-4 (S26 to S28). If the file is not infected, the process returns to S22.
[0041]

When it is determined in S28 that the file is suspected of being infected with a virus, and the operator is prompted to press the clean button 13-4, if the clean button 13-4 is pressed, the cleaning process is performed by the clean vaccine program loaded in the memory 17 (S29).
[0042]

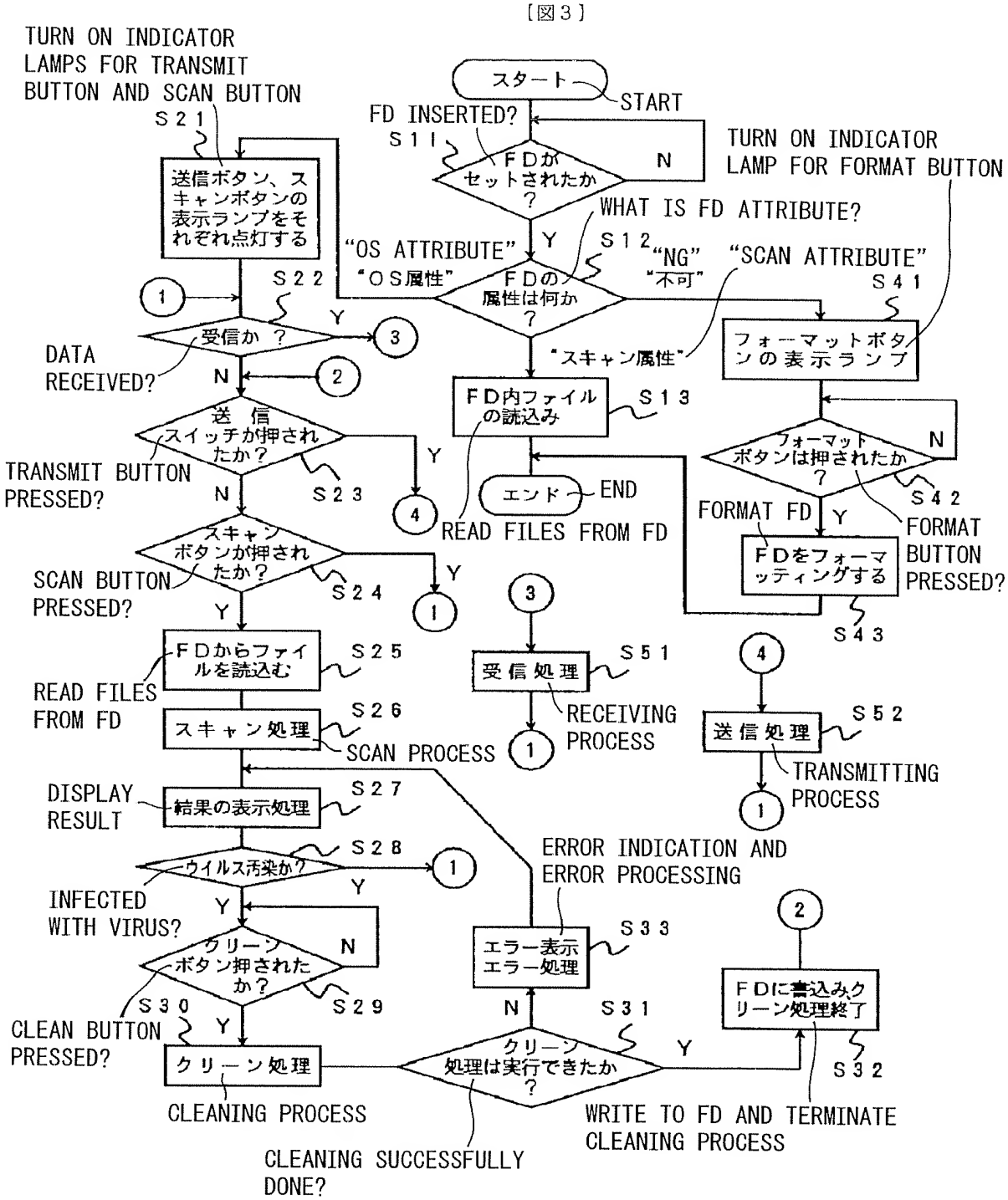
When the virus-infected file in the memory 17 has successfully been disinfected (which includes removing the

virus program portion) by performing the cleaning process, the disinfected file is written back to the floppy disk, and the cleaning process is terminated (S30 to S32). If the cleaning fails, an error indication lamp is turned on to indicate the occurrence of an error (error processing S33), and the process returns to S27 to retry the cleaning; if the cleaning still fails after retrying a predetermined number of times, the error indication lamp is flashed to indicate to the operator that the infected file cannot be disinfected (S33).

[Translation of the Drawing]

[FIG. 3]

[図3]



(19) JAPANESE PATENT OFFICE

PATENT ABSTRACTS OF JAPAN

(11) Publication number: **06168114 A**

(43) Date of publication of application: **14.06.94**

(51) Int. Cl **G06F 9/06**

(21) Application number: **04319530**

(22) Date of filing: **30.11.92**

(71) Applicant: **NIPPON SYST PROJECT:KK**

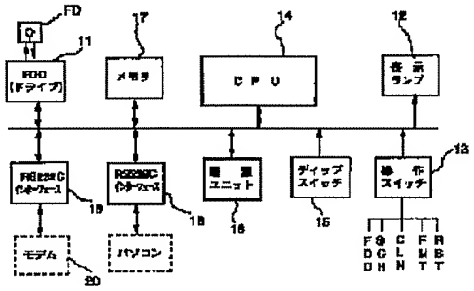
(72) Inventor: **TSUCHIYA TATSUHIKO**

(54) COMPUTER VIRUS DEFENSING DEVICE

(57) Abstract:

PURPOSE: To safely and easily prevent infection from a computer virus by checking whether a file read in from an external storage means is infected with the computer virus or not, thereby checking the computer virus before read to a computer file.

CONSTITUTION: The scan vaccine program read into a memory 17 is executed to check a file as the check object on a memory 17, and it is checked whether the computer virus is latent or not. If this file is suspicious or a specific virus is found as the check result, an indicator lamp corresponding to a clean button is flickered to inform that the file may be infected with the virus. When the clean button is depressed, the clean processing of a clean vaccine program is executed to make the file, which is infected with the virus, on the memory 17 harmless and when the clean processing is successful, the file made harmless is written in a floppy.



(19)日本国特許庁（ＪＰ）　(12)**公開特許公報**（Ａ）　(11)特許出願公開番号

特開平6－168114

(43)公開日　平成６年(1994)６月14日

(51)Int.Cl.[5]	識別記号	庁内整理番号	ＦＩ	技術表示箇所
Ｇ０６Ｆ　9/06	４５０　Ｚ	9367－5B		

審査請求　未請求　請求項の数５(全　９　頁)

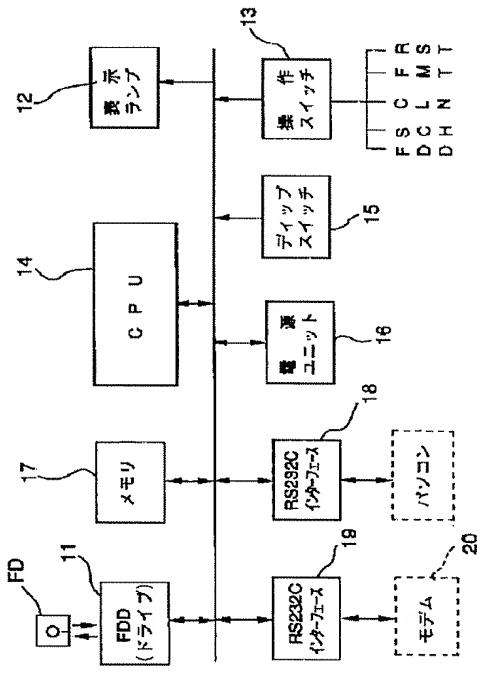
(21)出願番号　特願平4－319530

(22)出願日　平成４年(1992)11月30日

(71)出願人　592246565
株式会社日本システムプロジェクト
東京都渋谷区幡ヶ谷２－19－２
(72)発明者　土屋　達彦
東京都調布市布田１－22－１
(74)代理人　弁理士　鈴江　武彦

(54)【発明の名称】　コンピュータウイルス防御装置

(57)【要約】
【目的】本発明の目的はコンピュータにファイルを読み込ませる前にコンピュータウイルスのチェックを行うことができ、安全、且つ容易にコンピュータウイルスの感染を防止できるようにすることにある。
【構成】記憶媒体が着脱可能な外部記憶手段11と、外部記憶手段から読み込んだファイルについてコンピュータウイルス汚染のチェックを行う第１の機能および汚染ファイルについてコンピュータウイルスの影響を除くクリーン処理を行う第２の機能とを有する処理手段14と、このクリーン処理されたファイルを上記外部記憶手段に書き戻す手段14とを具備して構成した.



1

【特許請求の範囲】

【請求項１】　記憶媒体が着脱可能な外部記憶手段と、上記外部記憶手段から読み込んだファイルについてコンピュータウイルス汚染のチェックを行う第１の機能および汚染ファイルについてコンピュータウイルスの影響を除くクリーン処理を行う第２の機能とを有する処理手段と、

このクリーン処理されたファイルを上記外部記憶手段に書き戻す手段とを具備して構成したことを特徴とするコンピュータウイルス防御装置。

【請求項２】　記憶媒体が着脱可能な外部記憶手段と、上記外部記憶手段から読み込んだファイルについてコンピュータウイルス汚染のチェックを行い、結果を表示する第１の機能および汚染ファイルについてコンピュータウイルスの影響を除くクリーン処理を行う第２の機能とを有する処理手段と、

このクリーン処理されたファイルを上記外部記憶手段に書き戻す手段とを具備して構成したことを特徴とするコンピュータウイルス防御装置。

【請求項３】　記憶媒体が着脱可能な外部記憶手段と、上記外部記憶手段から読み込んだファイルについてコンピュータウイルス汚染のチェックを行う第１の機能および汚染ファイルについてコンピュータウイルスの影響を除くクリーン処理を行う第２の機能とを有する処理手段と、

このクリーン処理されたファイルを上記外部記憶手段に書き戻す手段と、

通信路を介して外部からのファイルを受信し、外部記憶手段に記録する通信手段と、を具備して構成したことを特徴とするコンピュータウイルス防御装置。

【請求項４】　記憶媒体が着脱可能な外部記憶手段と、上記外部記憶手段から読み込んだファイルについてコンピュータウイルス汚染のチェックを行い、結果を表示する第１の機能および汚染ファイルについてコンピュータウイルスの影響を除くクリーン処理を行う第２の機能とを有する処理手段と、

このクリーン処理されたファイルを上記外部記憶手段に書き戻す手段と、

通信路を介して外部からのファイルを受信し、外部記憶手段に記録する通信手段と、を具備して構成したことを特徴とするコンピュータウイルス防御装置。

【請求項５】　記憶媒体が着脱可能な外部記憶手段と、上記外部記憶手段から読み込んだファイルについてコンピュータウイルス汚染のチェックを行う第１の機能および汚染ファイルについてコンピュータウイルスの影響を除くクリーン処理を行う第２の機能とを有する処理手段と、

このクリーン処理されたファイルを上記外部記憶手段に書き戻す手段と、

通信路を介して外部からのファイルを受信し、外部記憶

2

手段に記録し、また、外部記憶手段からファイルを読出して通信路に送出する通信手段と、を具備して構成したことを特徴とするコンピュータウイルス防御装置。

【発明の詳細な説明】

【０００１】

【産業上の利用分野】本発明はウイルス予防機能を持たせたデータ端末装置に関するものである。

【０００２】

【従来の技術】近年、コンピュータを利用したデータ通信の発達に伴い、コンピュータプログラムやデータを破壊したりする所謂、コンピュータウイルス（悪さをするプログラム）が蔓延するようになり、自己のコンピュータシステムにおけるデータ等を保護するためにも、コンピュータウイルスの感染（侵入）を予防する必要が高まっている。

【０００３】コンピュータウイルスには、あるきっかけで悪さをする「論理爆弾(Logic bomb)」、データを破壊したり、他のプログラムには感染せず、単に自己をコピーして増やす「バクテリア／ラビット(Bacteria/Rabbit)」、複数のコンピュータを結ぶコンピュータネットワークを介して自己をコピーし、コンピュータネットワークを自力で伝わる「ワーム(Worm)」、ゲーム等のプログラムと見せ掛け、利用者を油断させて利用させ、その陰で悪さをする「トロイの木馬(Trojan horse)」と云った種類が知られている。

【０００４】いずれにせよ、このようなコンピュータウイルスはコンピュータシステムにとって全く不要のものであり、種別によってはデータを破壊したり、システムダウンを招くと云った悪影響を与えるものであるから、侵入を未然に防ぐ手立てが必要である。

【０００５】しかしながら、コンピュータウイルスはアプリケーションプログラムやユーティリティプログラム、ゲームプログラム、ツールプログラムなどと云った実行プログラムに潜んでいたり、システムファイルやオーバレイファイルに潜んでいたり、あるいはネットワークを介して感染するなど、水際で阻止することが難しい。

【０００６】そのため、一般的な防御策としては、利用しようとするソフトウェアに対して、ウイルスチェック用のプログラムを実行させて、ウイルス感染を調べ、ウイルスに感染していたならば、そのウイルス駆除用のプログラムを実行させて、無害化したり、除去したりしてから使用すると云った手法をとるのが一般的である。

【０００７】

【発明が解決しようとする課題】上述の如く、コンピュータウイルスはウイルスに感染したプログラムを使用したり、コンピュータ通信などによって自己のコンピュータシステムに感染する。そして、その結果、様々な悪影響をコンピュータシステムに与える。コンピュータウイルスの侵入を防ぐには、信用のおけるプログラムのみを

使用すれば良いわけであるが、コンピュータネットワークを介して感染するものがあるなど、完璧を期するに至らず、思わぬところでウイルス感染を招く。また、コンピュータ通信によって侵入するウイルスは防ぎようがないのが現状である。

【０００８】また、現状ではウイルス感染チェックのためには、ファイルを一旦、コンピュータシステムに取り込み、ファイル内容を調べなくてはならず、その際に、ウイルスに感染する危険が大きい。

【０００９】つまり、ウイルス感染チェックは少なくともフロッピレベルか、外部記憶装置レベルで行わねばならず、このような外部記憶装置に記憶された被疑ファイルを読出し、そのファイル容量変化や、日付、あるいはデータ列をチェックすることで、疑わしいものを知る。その際、コンピュータのメインメモリに少なくともファイルの一部は読み込まれることから、たとえ、その読み込んだファイルを実行しないにせよ、メインメモリに読み込まれることによってコンピュータシステムの他のファイルに感染する心配は完全には拭いきれない。また、ワームではコンピュータネットワーク上ではい回り、感染することから、現状ではこれを排除することができない。

【００１０】そこで、この発明の目的とするところは、コンピュータにファイルを読み込ませる前にコンピュータウイルスのチェックを行うことができ、安全、且つ容易にコンピュータウイルスの感染を防止できるようにしたコンピュータウイルス防御装置を提供することにある。

【００１１】

【課題を解決するための手段】上記目的を達成するため、本発明は次のように構成する。すなわち、記憶媒体が着脱可能な外部記憶手段と、上記外部記憶手段から読み込んだファイルについてコンピュータウイルス汚染のチェックを行う第１の機能および汚染ファイルについてコンピュータウイルスの影響を除くクリーン処理を行う第２の機能とを有する処理手段と、このクリーン処理されたファイルを上記外部記憶手段に書き戻す手段とを具備して構成した。

【００１２】更には、通信路を介して外部からのファイルを受信し、外部記憶手段に記録する通信手段を設けた。また、更には、通信手段には外部記憶手段からファイルを読出して通信路に送出する送信機能を付加した。

【００１３】

【作用】上記の構成において、処理手段は外部記憶手段から読み込んだファイルについてコンピュータウイルス汚染のチェックを行い、汚染ファイルであるか否かを調べ、汚染ファイルの疑いのあるときは、そのチェックしたファイルに対してコンピュータウイルスの影響を除くクリーン処理を行う。そして、書き戻す手段はこのクリーン処理されたファイルを上記外部記憶手段に書き戻す。

【００１４】通信手段を設けた構成とした場合には、通信路を介して外部からのファイルを受信し、外部記憶手段に記録することができ、この外部記憶手段に記録した受信ファイルをコンピュータウイルス汚染のチェック並びにクリーン処理することができ、また、通信手段に外部記憶手段からファイルを読出して通信路に送出する送信機能を付加した場合には、コンピュータウイルス汚染の影響の心配がないクリーン処理したファイルを送信することができる。

【００１５】従って、コンピュータにファイルを読み込ませる前にコンピュータウイルスのチェックを行うことができ、安全、且つ容易にコンピュータウイルスの感染を防止できるようになる。

【００１６】

【実施例】以下、本発明の一実施例について、図面を参照して説明する。本発明によるコンピュータウイルス防御装置の構成を説明する。本発明によるコンピュータウイルス防御装置１０は独立した装置であり、本装置単独で動作可能であると共に、通信用のインタフェースを備えて、パソコンなどのホストシステムに端末として接続して使用することも可能である。

【００１７】本発明によるコンピュータウイルス防御装置１０は図１に示すように、フロッピドライブ１１と複数の操作ボタン１３－１～１３－５、表示ランプ１２－１～１２－７を有している。

【００１８】操作ボタンのうち、１３－１はシステムリセットを行うためのリセットボタン（ＲＳＴ）、１３－２はデータ送信ボタン（ＦＤＤ）、１３－３はスキャンボタン（ＳＣＮ）、１３－４はクリーンボタン（ＣＬＮ）、１３－５はフロッピ・フォーマットボタン（ＦＭＴ）であり、これら各ボタンに対応して一つづつ表示ランプ１２－１～１２－５が設けられている。

【００１９】また、この他、動作ランプ１２－６、エラー表示ランプ１２－７がある。図示しないが、さらにコンピュータウイルス防御装置１０の背面にはＲＳ２３２Ｃのコネクタと、機能設定用のディップスイッチが設けられている。

【００２０】機能設定用のディップスイッチとしては、ＲＳ２３２Ｃのボーレイトなどをはじめとする通信条件の他、本装置１０を使用するに際しての各種条件などを設定することができる。また、リセットボタン１３－１は本装置１０が暴走したり、エラーを起こしたときに、システムリセットするためのものである。

【００２１】本装置１０は電源コードをコンセントに差し込んで、スイッチをオンさせることにより電力を供給して動作状態にすることができ、また、内部の電池電源により内部メモリのバックアップを行う構成としてある。なお、商用電源を常時通電させておく構成とした装置の場合は、電源断時のバックアップのために、大容量

のコンデンサを設けておくことにより、そのチャージ電荷を利用して６時間程度はメモリ内の記憶データを失わないようにすると云った手法を利用することができる。また、内部メモリにはフラッシュメモリを使用することもでき、この場合は特に内部メモリのバックアップは必要ない。

【００２２】図２は本装置１０の構成を示すシステムブロック図である。図において、１１は前記フロッピ・ディスク・ドライブ（ＦＤＤ）であり、１２は前記表示ランプ、１４は本装置の制御の中枢を担うマイクロプロセッサ（ＣＰＵ）である。また、１５は機能設定用のディップスイッチであり、１６は電源ユニットであり、また、１３は操作スイッチであって、図１で説明したシステムリセットボタン（ＲＳＴ）１３－１、データ送信ボタン（ＦＤＤ）１３－２、スキャンボタン（ＳＣＮ）１３－３、クリーンボタン（ＣＬＮ）１３－４、フロッピ・フォーマットボタン（ＦＭＴ）１３－５に相当する。

【００２３】１７はメモリであり、１８および１９はそれぞれシリアル・通信用のインタフェースであるＲＳ２３２Ｃインタフェースであり、２０は一方のＲＳ２３２Ｃインタフェース１８に接続されたモデムである。また、他方のＲＳ２３２Ｃインタフェース１９には例えばパソコンのＲＳ２３２Ｃインタフェースに接続することで、パソコンとデータ授受することができる。

【００２４】メモリ１７はＲＡＭおよびＲＯＭからなり、ＲＯＭにはフロッピ・ディスク（ＦＤ）のデータフォーマットをチェックして属性を調べる機能、処理モードに応じてデータ処理および各種制御を実施するためのプログラム、エラー表示ランプやその他の表示ランプの点灯制御等のプログラムを有している。このプログラムはＣＰＵ１４に実行させ、各種制御を実現する。

【００２５】そして、この制御プログラムとして、フロッピ・ディスク・ドライブ１１にフロッピ・ディスク（ＦＤ）が挿入された場合、そのＦＤの属性を調べて、その属性が本システム用として提供されるウイルスチェック用のスキャンプログラム属性である場合およびワクチンプログラム属性である場合には、そのプログラムの読み込みを行ってメモリ１７におけるＲＡＭ上の所定の実行プログラム記憶領域に書き込むと云った処理をして終了し、待機状態になり、また、当該システムで扱うことのできるＯＳ（オペレーションシステムタ）対応のフォーマットがなされていないフロッピ・ディスク（アンフォーマットの時も含む）であった場合はフォーマットモードになり、フォーマットボタン１３－５対応のランプ１２－５を点灯させてフォーマット操作が可能であることを示し、フォーマットボタン１３－５が押されれば、ＦＤに対して当該システムで扱うことのできる所定ＯＳ対応のフォーマッティングを行ってから終了し、待機状態になり、挿入されたＦＤが当該システムで扱うことのできるＯＳ対応のフォーマットがなされたフロッピ・ディスクであった場合は送信ボタン１３－２対応のランプおよびスキャンボタン１３－３対応のランプ対応のランプの点灯を行い、送受信およびスキャン（ウイルスチェック）操作が可能であることを示し、いずれかのランプで表示したボタンのいずれかが操作されればそれぞれ対応の処理を行う。

【００２６】また、この状態ではいずれのボタンも押されず、モデムあるいはＲＳ２３２Ｃ等の通信インタフェースを介して相手方からデータの受信があったときは受信モードとなり、受信のためのプロトコル制御を行って相手回線とリンクさせた後、送られてくるデータを取り込み、メモリ１７におけるＲＡＭ上の所定のデータ記憶領域に書き込むと云った処理を行う。

【００２７】ＲＡＭ上に書き込まれたデータは、逐次ＦＤに転送して書き込むが、書き込み指示ボタンを設けた場合には、この書き込み指示ボタンの操作によりＦＤに転送して書き込むように処理する機能を設けることもできる。

【００２８】このように、ＦＤが挿入されると、そのＦＤの属性をチェックし、スキャンおよびワクチンプログラム属性の場合は当該プログラムを読み込み、当該属性以外で、特定ＯＳフォーマットの場合はデータ送信表示ランプおよびスキャンボタン対応のランプを点灯させ、データの送受信とデータのウイルスチェック操作が可能であることを表示させ、いずれの属性でもないあるいはアンフォーマットのフロッピ・ディスクが挿入された場合は、フォーマットボタン１３－５対応の表示ランプを点灯させ、どのモードが使用可能であるかをユーザに知らせることができる機能とを持たせる共に、操作可能なボタンが操作された時はそれ対応の処理を実施し、また、ボタンが押されずに受信があったときは受信処理をしてＦＤに転送すると云った処理をする機能を持たせてある。

【００２９】スキャン処理はメモリ１７に読み込まれたスキャンワクチンプログラムを実行して、メモリ１７上にあるチェック対象のファイルをチェックし、コンピュータウイルスが潜んでいるか否かを調べる処理であり、チェックの結果、疑わしいものの場合および特定のウイルスが発見された場合はクリーンボタン１３－４に対応する表示ランプ１２－４を点滅してウイルスに汚染された可能性のあるファイルであることを知らせ、クリーンボタン１３－４を押すように促すと共に、クリーンボタン１３－４が押されたならば、クリーンワクチンプログラムによるクリーン処理を実行して、当該メモリ１７上にあるウイルス汚染ファイルの無害化（ウイルスプログラム部分の除去を含む）を行わせ、クリーン処理が成功したならば無害化されたファイルをフロッピに書き込むと云った処理である。

【００３０】また、上記ＲＡＭはプログラムの作業領域、通信用のバッファなどにも使用される。フロッピ・

ディスク・ドライブ１１はフロッピ・ディスクの挿抜を検知する機能を有している。

【００３１】なお、本システムにおいては、スキャンワクチンプログラムや、クリーンワクチンプログラムを提供するスキャン属性のフォームのフロッピと、ＭＳ－ＤＯＳやＤＯＳ／Ｖなどの、このシステムで取り扱うことのできる特定ＯＳのフォーマットによるフロッピについて、その属性を読み取って上述のような特定処理を行うようにしてある。

【００３２】スキャンワクチンプログラムは各種コンピュータウイルスのチェックを行うプログラムであり、現在知られている各種コンピュータウイルスのコード列や、有名ソフトウェアの各種ファイル長、ファイルスタンプ、ファイル属性等の情報を予め用意してあり、これらの情報を手掛かりに比較照合してコンピュータウイルスを特定したり、コンピュータウイルス汚染ファイルの疑いの有無をチェックしたりするプログラムおよびデータである。

【００３３】クリーンワクチンプログラムは特定のコンピュータウイルスに感染したファイルに対して、そのコンピュータウイルスを無害化したり、コンピュータウイルスのプログラムルーチンを取り除いたりする駆除プログラムであり、既知のコンピュータウイルスそれぞれに対してのものが用意される。

【００３４】次に上記構成の本装置に作用を図３のフローチャートを参照して説明する。本装置ではフロッピ・ディスク・ドライブ１１にフロッピ・ディスクが挿入されると、ＣＰＵ１４はそのフロッピの属性を調べる（Ｓ１１，Ｓ１２）。そして、その属性に応じて次のような処理を実施する。

【００３５】今、挿入されたフロッピ・ディスクが、スキャン属性であるとＣＰＵ１４が認識した場合、ＣＰＵ１４はそのフロッピ・ディスクのプログラムファイルやデータファイルを読み込み、メモリ１７上の特定の領域（スキャンプログラムはスキャンプログラム用の領域、クリーンプログラムはクリーンプログラム用の領域）に格納する（Ｓ１３）。そして、読み込むと終了する。

【００３６】一方、挿入されたフロッピ・ディスクが、スキャン属性以外の属性で本システムで扱うことのできる特定のＯＳ属性のフロッピ・ディスクであるとＣＰＵ１４が認識した場合、ＣＰＵ１４は送信ボタン１３－２対応のランプおよびスキャンボタン１３－３対応のランプの点灯を行い、送受信およびスキャン（ウイルスチェック）の操作が可能であることをオペレータに知らせる（Ｓ２１）。次にＣＰＵ１４はいずれかのランプで表示したボタンのいずれかが操作されるかを監視する（Ｓ２２～Ｓ２４）。

【００３７】この状態ではいずれのボタンも押されず、モデムあるいはＲＳ２３２Ｃ等の通信インタフェースを介して相手方からデータの受信があったときは受信モードとなり、受信のためのプロトコル制御を行って相手回線とリンクさせた後、送られてくるデータを取り込み、メモリ１７におけるＲＡＭ上の所定のデータ記憶領域（作業領域）に書き込むと云った処理を行う（Ｓ５１）。この状態ではボタン操作はリセットを除いて受付けない。また、この受信処理ではメモリ１７に書き込んだ受信データはフロッピ・ディスクに書き込む。この受信処理が終わると、ＣＰＵ１４は再び、いずれかのランプで表示したボタンのいずれかが操作されるかを監視する（Ｓ２３～Ｓ２５）。

【００３８】送信ボタン１３－２が押されれば、送信処理に移る（Ｓ５２）。この送信処理では送信のためのプロトコル制御を行ってからフロッピ・ディスクに格納されたファイルを読み込んでＲＳ２３２Ｃインタフェースまたはモデムに送る。

【００３９】スキャンボタン１３－３が押されれば、スキャン処理に移る（Ｓ２５）。この処理ではＣＰＵ１４はそのフロッピ・ディスクのプログラムファイルやデータファイルを読み込み、メモリ１７上の特定の領域（作業用の領域）に格納する。これはファイルがある場合であり、ファイルが存在しない場合は終了する。

【００４０】ファイルが読み込まれたならば、メモリ１７に読み込まれているスキャンプログラムを実行して、メモリ１７上にあるチェック対象のファイルをチェックし、コンピュータウイルスが潜んでいるか否かを調べる。チェックの結果、疑わしいものの場合および特定のウイルスが発見された場合はクリーンボタン１３－４に対応する表示ランプ１２－４を点滅してウイルスに汚染された可能性のあるファイルであることを知らせ、クリーンボタン１３－４を押すように促す（Ｓ２６～Ｓ２８）。ファイルが汚染されていなければＳ２２に戻る。

【００４１】Ｓ２８における汚染判定の結果、汚染の可能性があってクリーンボタン１３－４を押すように促された状態のときに、クリーンボタン１３－４を押せば、メモリ１７上のクリーンワクチンプログラムによるクリーン処理を実行する（Ｓ２９）。

【００４２】クリーン処理を実行した結果、当該メモリ１７上にあるウイルス汚染ファイルの無害化（ウイルスプログラム部分の除去を含む）が成功したならば無害化されたファイルをフロッピ・ディスクに書き戻し、クリーン処理を終了する（Ｓ３０～Ｓ３２）。クリーン処理が失敗ならば、エラー表示ランプを点灯してエラー表示し（エラー処理Ｓ３３）、Ｓ２７に戻って数回のリトライを可能にし、規定回のリトライによってもクリーン処理が失敗ならば、エラー表示ランプを点滅させて汚染されているファイルが無害化できないことをオペレータに知らせる（Ｓ３３）。

【００４３】汚染されているファイルが無害化できたときは、無害化されたファイルをフロッピ・ディスクに書き戻し、クリーン処理を終了して（Ｓ３０～Ｓ３２）、

送信ランプを点灯させてＳ２２に戻る。

【００４４】Ｓ１２のフロッピ・ディスク属性チェックの結果、アンフォーマット・ディスク若しくは本システムで扱えないＯＳのフォーマット・ディスクであるときは、ＣＰＵ１３はフロッピ・フォーマットボタン（ＦＭＴ）１３－５に対応するランプ１２－５のみを点灯させ（Ｓ４１）、フロッピ・フォーマットが可能であることをオペレータに知らせる。

【００４５】フロッピ・フォーマットボタン（ＦＭＴ）１３－５が押されると（Ｓ４２）、フロッピ・フォーマットモード（以下、ＦＭＴモードと称する）に移行し、フロッピ・ディスク・ドライブ１１に挿入されたフロッピ・ディスクを特定ＯＳ用の形式のフォーマットでフォーマッティングする処理を実施する（Ｓ４３）。そして、終了したならば待機状態になる。待機状態ではフロッピ・ディスクを入れ替えることで上述の動作を最初から始める。

【００４６】本装置では、クリーン処理を済ませれば、フロッピ・ディスクにクリーン処理済みのファイルを書き込むことができ、この書き込みを元のファイル名と同じファイル名で上書きすれば、フロッピ・ディスクには無害化されたファイルが残り、このフロッピ・ディスクをパソコンにセットして読み込むことで、安全なファイルをパソコンに供給できる。また、通信インタフェースを介してこのフロッピ・ディスクのファイルを伝送すれば、相手先に安全なファイルを供給できる。

【００４７】このように、上述の実施例によれば、フロッピ・ディスク・ドライブ１１にＦＤを挿入すると、ＣＰＵ１４はそのＦＤを読みに入り、ＦＤのフォーマットからその属性を判定して、その属性からとり得るモードを判別し、そのモードでの操作できるボタン対応の表示ランプを点灯させるようにして、操作をわかり易くし、ファイルが書き込まれているフロッピ・ディスクが装着された状態で、スキャンワクチンプログラムによるスキャン処理を行うと、コンピュータウイルス汚染が疑われるファイルについて、さらにクリーン処理を行うことができるようにし、コンピュータウイルスの影響がない状態にしてファイルをフロッピ・ディスクに書き戻すようにしたり、通信インタフェースを介してパソコンなどのホストシステムに転送できるようにしたり、また、本装置を介してウイルスチェックを行って通信を行うようにすることを可能にしたので、パソコンやホストコンピュータなどにファイルを読み込ませる前にコンピュータウイルスのチェックを行うことができ、安全、且つ容易にコンピュータウイルスの感染を防止できるようになる。

【００４８】なお、本発明は上記し、且つ、図面に示す実施例に限定することなく、その要旨を変更しない範囲内で適宜変更して実施し得ることはもちろんである。例えば、上記実施例では記憶媒体としてフロッピ・ディスクを使用する例を示したが、これに限るものではなく、

メモリカード等のＩＣカード等の他の記憶媒体を利用して実施可能である。

【００４９】また、本装置においては、スキャンワクチンプログラムとクリーンワクチンプログラムはフロッピ（他のメディアでも可能）で供給し、メモリ１７に読み込ませて使用する形態を採用しているので、定期的にバージョンアップして常に最新のコンピュータウイルスに対処できるようにすることが可能である。

【００５０】さらに、本装置においては、表示ランプを複数有しており、これらの表示パターンをウイルスの種別に対応して変えて表示させるようにすることもでき、このようにすれば、どのようなウイルスに汚染されていたかがわかるようになる。また、キャラクタ表示部を設けて、このような情報をキャラクタ表示するようにすることも容易に実現可能である。

【００５１】以上、本発明は記憶媒体が着脱可能な外部記憶手段と、上記外部記憶手段から読み込んだファイルについてコンピュータウイルス汚染のチェックを行う第１の機能および汚染ファイルについてコンピュータウイルスの影響を除くクリーン処理を行う第２の機能とを有する処理手段と、このクリーン処理されたファイルを上記外部記憶手段に書き戻す手段とを具備して構成した。

【００５２】更には、通信路を介して外部からのファイルを受信し、外部記憶手段に記録する通信手段を設けた。また、更には、通信手段には外部記憶手段からファイルを読出して通信路に送出する送信機能を付加した。

【００５３】そして、上記の構成において、処理手段は外部記憶手段から読み込んだファイルについてコンピュータウイルス汚染のチェックを行い、汚染ファイルであるか否かを調べ、汚染ファイルの疑いのあるときは、そのチェックしたファイルに対してコンピュータウイルスの影響を除くクリーン処理を行い、そして、書き戻す手段はこのクリーン処理されたファイルを上記外部記憶手段に書き戻す。

【００５４】また、通信手段を設けた構成とした場合には、通信路を介して外部からのファイルを受信し、外部記憶手段に記録することができ、この外部記憶手段に記録した受信ファイルをコンピュータウイルス汚染のチェック並びにクリーン処理することができるようになり、また、通信手段に外部記憶手段からファイルを読出して通信路に送出する送信機能を付加した場合には、コンピュータウイルス汚染の影響の心配がないクリーン処理したファイルを送信することができるようになる。

【００５５】従って、本発明によれば、コンピュータにファイルを読み込ませる前にコンピュータウイルスのチェックを行うことができ、安全、且つ容易にコンピュータウイルスの感染を防止できるようになる。

【００５６】

【発明の効果】以上、詳述したようにこの発明によれば、コンピュータにファイルを読み込ませる前にコンピ

11

ュータウイルスのチェックを行うことができ、安全、且つ容易にコンピュータウイルスの感染を防止できるようになるコンピュータウイルス防御装置を提供できる。

【図面の簡単な説明】

【図１】本発明の一実施例を示すシステム外観図。

【図２】本発明による装置のシステムブロック図。

【図３】本発明による装置の動作を説明するためのフローチャート。

【符号の説明】

１０…コンピュータウイルス防御装置本体　＊10

12

＊１１…フロッピディスクドライブ（ＦＤＤ）

１２－１～１２－７…表示ランプ

１３－１～１３－５…各種操作用のボタン（操作スイッチ）

１４…マイクロプロセッサ（ＣＰＵ）

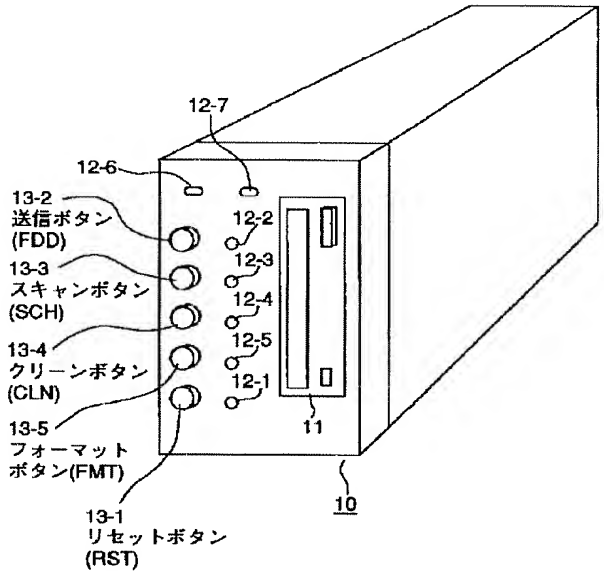
１５…機能設定用のディップスイッチ

１６…電源ユニット

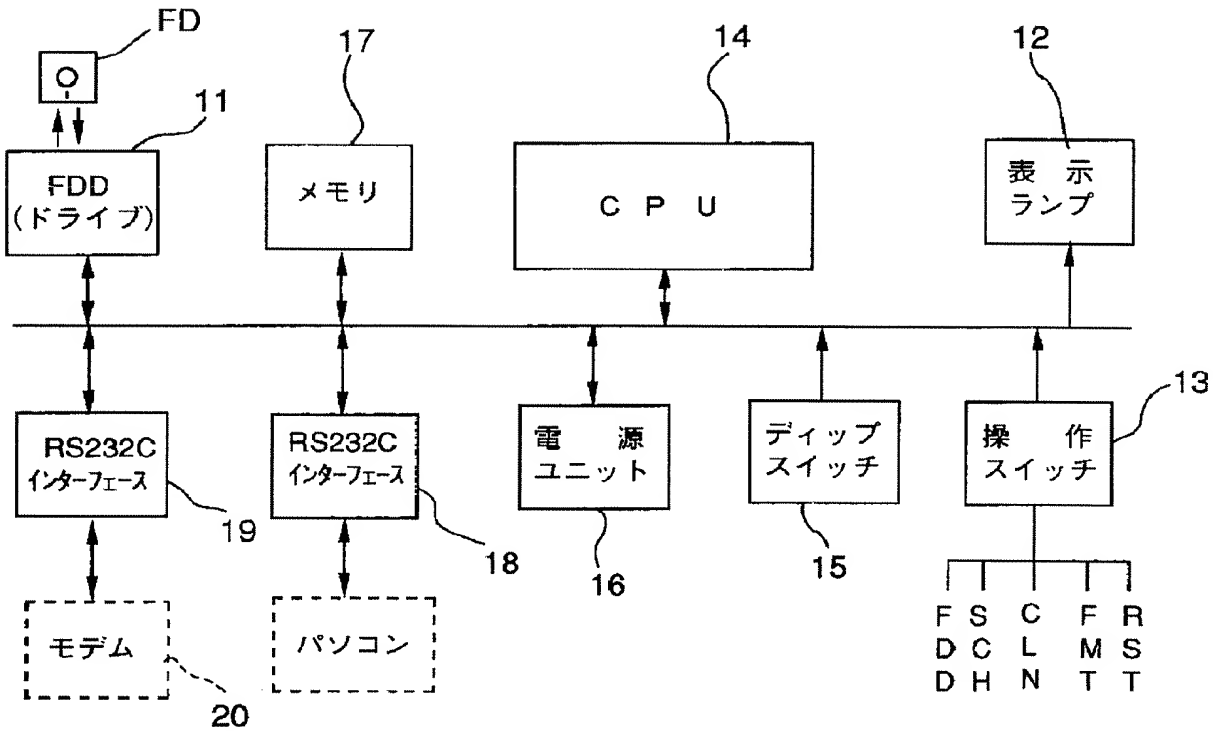
１７…メモリ

１８，１９…ＲＳ２３２Ｃインタフェース

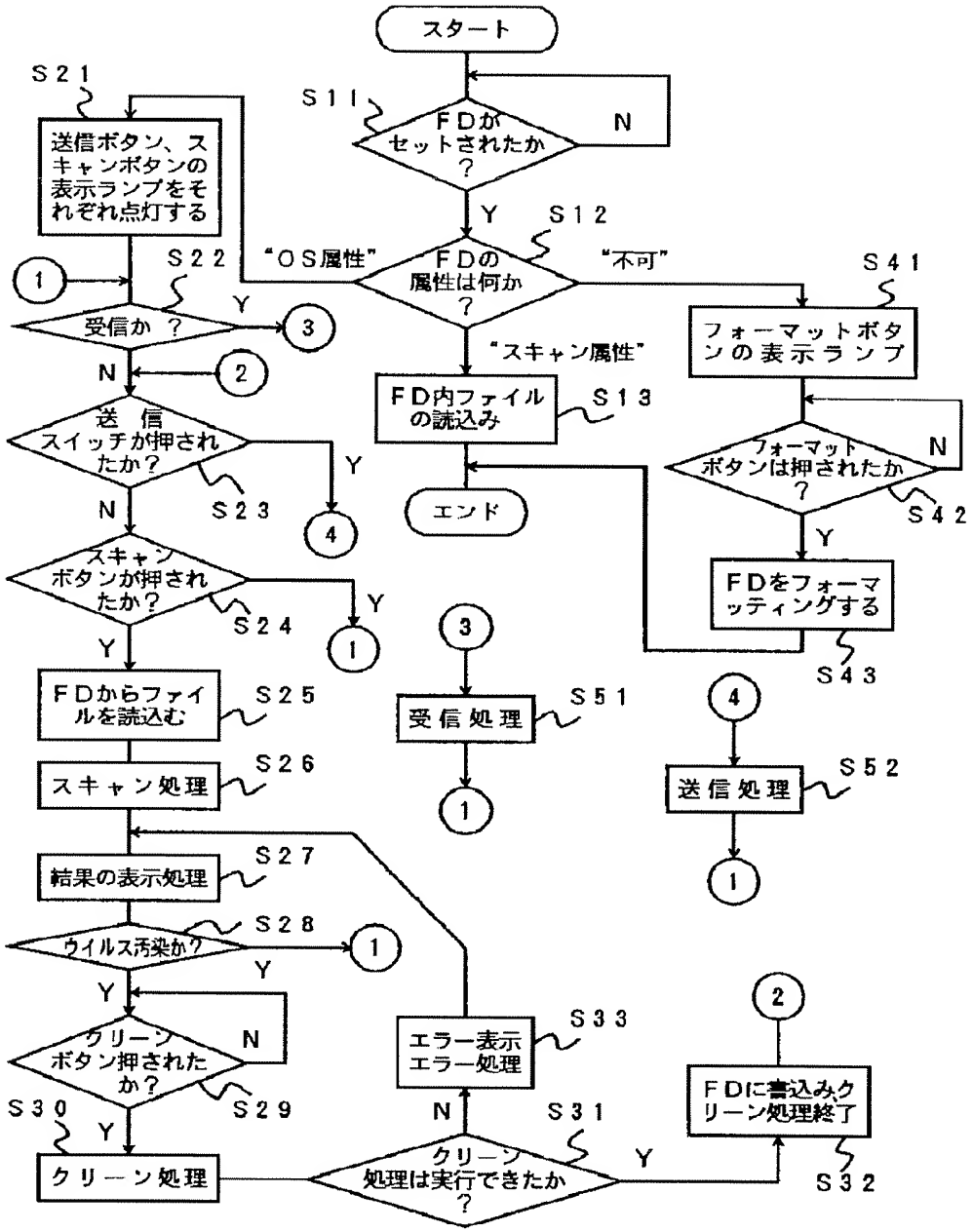
【図１】



【図２】


FD
11
FDD
(ドライブ)
17
メモリ
14
C P U
12
表　示
ランプ
13
RS232C
インターフェース
19
RS232C
インターフェース
18
電　源
ユニット
16
ディップ
スイッチ
15
操　作
スイッチ
モデム
20
パソコン
FDD
FSCH
CLN
FMT
RST

【図３】


スタート
S11
FDがセットされたか？
N
Y
S12
FDの属性は何か？
"OS属性"
"スキャン属性"
"不可"
S41
フォーマットボタンの表示ランプ
FD内ファイルの読込み
S13
エンド
フォーマットボタンは押されたか？
N
S42
Y
FDをフォーマッティングする
S43
S21
送信ボタン、スキャンボタンの表示ランプをそれぞれ点灯する
S22
受信か？
Y
N
送信スイッチが押されたか？
S23
スキャンボタンが押されたか？
S24
FDからファイルを読込む
S25
スキャン処理
S26
結果の表示処理
S27
ウイルス汚染か？
S28
クリーンボタン押されたか？
S29
S30
クリーン処理
受信処理
S51
送信処理
S52
エラー表示エラー処理
S33
クリーン処理は実行できたか？
S31
FDに書込みクリーン処理終了
S32
1
2
3
4